

# WPA配置概述

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景理論](#)

[慣例](#)

[設定](#)

[網路EAP或使用EAP的開放式身份驗證](#)

[CLI組態](#)

[GUI配置](#)

[驗證](#)

[疑難排解](#)

[疑難排解程式](#)

[指令疑難排解](#)

[相關資訊](#)

## 簡介

本文檔提供了Wi-Fi保護訪問(WPA)配置示例，WPA是Wi-Fi聯盟成員使用的臨時安全標準。

## 必要條件

### 需求

嘗試此組態之前，請確保符合以下要求：

- 全面瞭解無線網路和無線安全問題
- 可擴展身份驗證協定(EAP)安全方法知識

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS®軟體型存取點(AP)
- Cisco IOS軟體版本12.2(15)JA或更新版本**注意**：最好使用最新的Cisco IOS軟體版本，即使Cisco IOS軟體版本12.2(11)JA及更高版本支援WPA。若要取得最新的Cisco IOS軟體版本，請參閱[下載](#)(僅限[註冊](#)客戶)。
- 相容WPA的網路介面卡(NIC)及其WPA相容客戶端軟體

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 背景理論

無線網路（例如WEP）的安全功能較弱。Wi-Fi聯盟（或WECA）行業團隊為無線網路設計了一個下一代臨時安全標準。該標準提供在IEEE組織批准802.11i標準之前針對弱點的防禦。

此新方案基於當前EAP/802.1x身份驗證和動態金鑰管理，並新增了更強大的密碼加密。客戶端裝置和身份驗證伺服器建立EAP/802.1x關聯後，AP和相容WPA的客戶端裝置之間會協商WPA金鑰管理。

思科AP產品還提供混合配置，其中基於WEP的傳統EAP客戶端（具有傳統或無金鑰管理）與WPA客戶端協同工作。此配置稱為遷移模式。遷移模式允許分階段遷移到WPA。本文檔不涉及遷移模式。本文檔提供了純WPA安全網路的大綱。

除了企業或企業級別的安全問題外，WPA還提供預共用金鑰版本(WPA-PSK)，用於小型辦公室、家庭辦公室(SOHO)或家庭無線網路。Cisco Aironet客戶端實用程式(ACU)不支援WPA-PSK。Microsoft Windows中的無線零配置實用程式支援大多數無線卡的WPA-PSK，這些實用程式也是如此：

- Meetinghouse Communications的AEGIS客戶端註：請參閱[Meetinghouse AEGIS產品系列的EOS和EOL公告](#)。
- Funk Software的Odyssey客戶端注意：請參閱[Juniper Networks客戶支援中心](#)。
- 某些製造商的原始裝置製造商(OEM)客戶端實用程式

在以下情況下，可以配置WPA-PSK：

- 在加密管理器頁籤上，將加密模式定義為密碼臨時金鑰完整性協定(TKIP)。
- 您可以在GUI的Service Set Identifier(SSID)Manager頁籤上定義身份驗證型別、使用經過身份驗證的金鑰管理和預共用金鑰。
- 伺服器管理器頁籤上不需要配置。

若要透過指令行介面(CLI)啟用WPA-PSK，請輸入以下命令。從組態模式開始：

```
AP(config)#interface dot11Radio 0
AP(config-if)#encryption mode ciphers tkip
AP(config-if)#ssid ssid_name
AP(config-if-ssid)#authentication open
AP(config-if-ssid)#authentication key-management wpa
AP(config-if-ssid)#wpa-psk ascii pre-shared_key
```

**注意：**本節僅提供與WPA-PSK相關的配置。本節中的配置只是向您介紹如何啟用WPA-PSK，而不是本文檔的重點。本文說明如何配置WPA。

## 慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

## 設定

WPA基於當前的EAP/802.1x方法。本文檔假定在新增配置以使用WPA之前，您有一個輕量EAP(LEAP)、EAP或受保護的EAP(PEAP)配置。

本節提供用於設定本檔案中所述功能的資訊。

**註：** 使用[Command Lookup Tool](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

## 網路EAP或使用EAP的開放式身份驗證

在任何基於EAP/802.1x的身份驗證方法中，您可能會問Network-EAP和Open authentication with EAP之間有何區別。這些專案引用管理和關聯資料包報頭中的Authentication Algorithm欄位中的值。大多數無線客戶端製造商將此欄位設定為值0（開放式身份驗證），然後表示希望在關聯過程後期進行EAP身份驗證。Cisco設定值的方式與使用Network EAP標誌開始關聯時不同。

使用此清單指示您的網路是否有以下客戶端的身份驗證方法：

- Cisco clients — 使用Network-EAP。
- 第三方客戶端（包括符合Cisco Compatible Extensions [CCX]標準的產品） — 使用Open authentication with EAP。
- 思科和第三方客戶端的組合 — 同時選擇Network-EAP和Open authentication with EAP。

## CLI組態

本檔案會使用以下設定：

- 存在並正常工作的LEAP配置
- 適用於Cisco IOS軟體型AP的Cisco IOS軟體版本12.2(15)JA

```
AP
apl#show running-config
Building configuration...
.
.
.
aaa new-model
!
aaa group server radius rad_eap
server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers tkip
!--- This defines the cipher method that WPA uses. The
TKIP !--- method is the most secure, with use of the Wi-
Fi-defined version of TKIP. ! ssid WPAalabap1200
```

```

authentication open eap eap_methods
!--- This defines the method for the underlying EAP when
third-party clients !--- are in use. authentication
network-eap eap_methods
!--- This defines the method for the underlying EAP when
Cisco clients are in use. authentication key-
management wpa
!--- This engages WPA key management. ! speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 rts threshold 2312
channel 2437 station-role root bridge-group 1 bridge-
group 1 subscriber-loop-control bridge-group 1 block-
unknown-source no bridge-group 1 source-learning no
bridge-group 1 unicast-flooding bridge-group 1 spanning-
disabled . . . interface FastEthernet0 no ip address no
ip route-cache duplex auto speed auto bridge-group 1 no
bridge-group 1 source-learning bridge-group 1 spanning-
disabled ! interface BVI1 ip address 192.168.2.108
255.255.255.0 !--- This is the address of this unit. no
ip route-cache ! ip default-gateway 192.168.2.1 ip http
server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server host 192.168.2.100 auth-port 1645 acct-
port 1646 key shared_secret !--- This defines where the
RADIUS server is and the key between the AP and server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip !! line con 0
line vty 5 15 ! end ! end

```

## GUI配置

完成以下步驟，以便為WPA配置AP:

1. 完成以下步驟以設定加密管理器：為TKIP啟用密碼。清除加密金鑰1中的值。將Encryption Key 2設定為Transmit Key。按一下「Apply-Radio#」。

The screenshot displays the configuration interface for a Cisco 1200 Access Point, specifically the 'Security: Encryption Manager' for radio0 802.11B. The 'Encryption Modes' section shows 'Cipher' selected, with 'TKIP' chosen from the dropdown menu. The 'Encryption Keys' section shows 'Encryption Key 2' selected. The 'Global Properties' section shows 'Broadcast Key Rotation Interval' set to 'Disable Rotation' and 'WPA Group Key Update' options. The page includes a navigation menu on the left and a footer with 'Copyright (c) 1997-2004 by Cisco Systems, Inc.'

2. 完成以下步驟以設定SSID管理器：從當前SSID清單中選擇所需的SSID。選擇適當的身份驗證方法。根據您使用的客戶端卡型別作出此決定。有關詳細資訊，請參閱本文檔的[網路EAP或使用EAP的開放式身份驗證](#)部分。如果EAP在新增WPA之前有效，則可能不需要更改。完成以下步驟以啟用金鑰管理：從Key Management下拉選單中選擇**Mandatory**。選中WPA覈取方塊。按一下「Apply-Radio#」。

The screenshot displays the configuration interface for a Cisco 1200 Access Point. The main heading is "Cisco 1200 Access Point". The left sidebar contains navigation menus for "HOME", "EXPRESS SET UP", "EXPRESS SECURITY", "NETWORK MAP", "ASSOCIATION", "NETWORK INTERFACES", "SECURITY", "SERVICES", "WIRELESS SERVICES", "SYSTEM SOFTWARE", and "EVENT LOG". The "SECURITY" menu is expanded, showing "Admin Access", "Encryption Manager", "SSID Manager", "Server Manager", "Local RADIUS Server", and "Advanced Security". The "SSID Manager" option is selected. The main content area is titled "Security: SSID Manager - Radio0-802.11B". It includes a "Current SSID List" with a table containing one entry: "WPAIabop1200". To the right of the table are fields for "SSID:" (WPAlabop1200), "VLAN:" (NONE), and "Network ID:" (0-4095). Below the table are "Delete-Radio0" and "Delete-All" buttons. The "Authentication Settings" section includes "Methods Accepted" with "Open Authentication" and "Network EAP" checked, and "Server Priorities" for both "EAP Authentication Servers" and "MAC Authentication Servers" set to "Use Defaults". The "Authenticated Key Management" section shows "Key Management" set to "Mandatory" and "WPA" checked. The "WPA Pre-shared Key" field is empty, and the "WPA" radio button is checked.

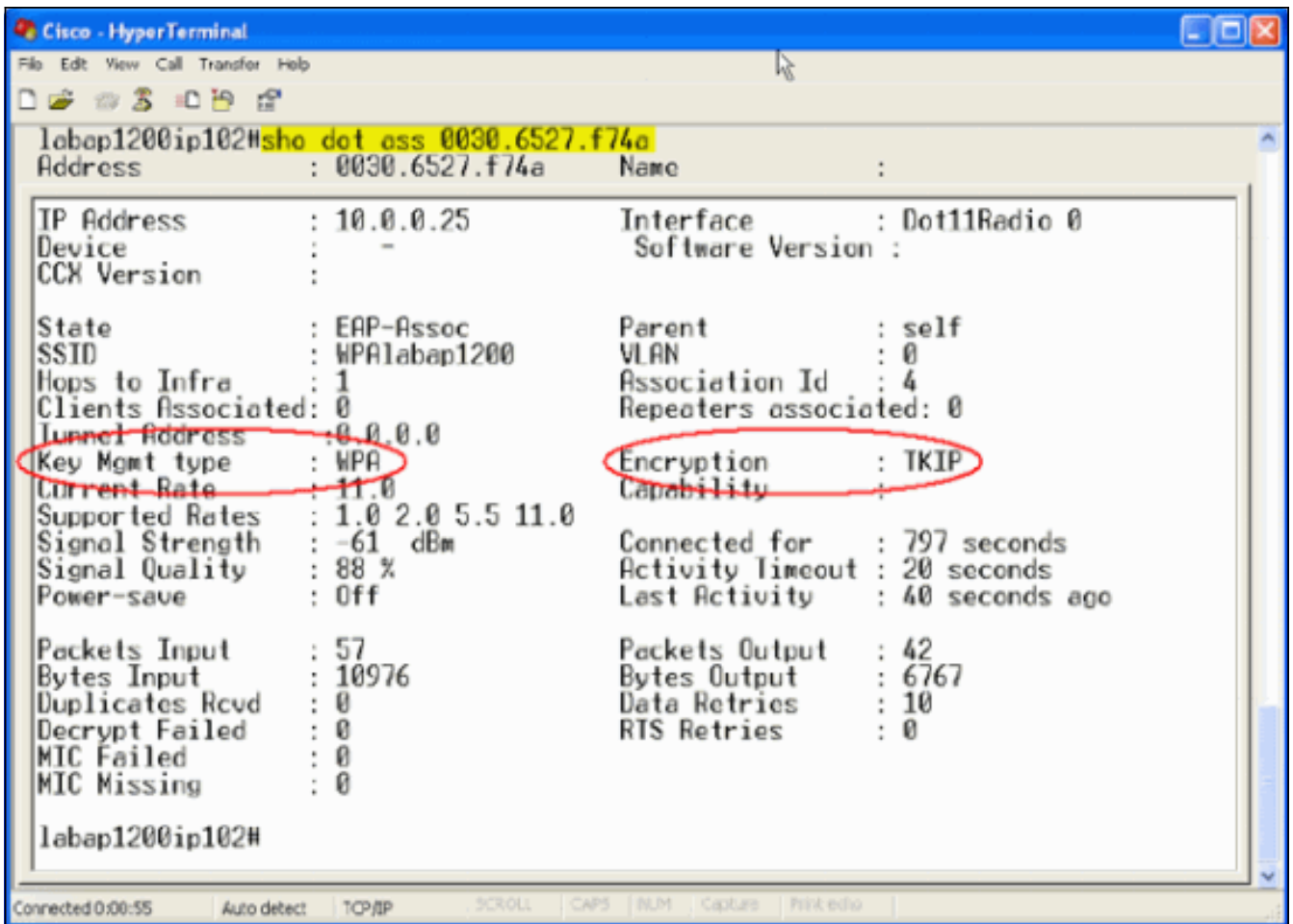
## 驗證

使用本節內容，確認您的組態是否正常運作。

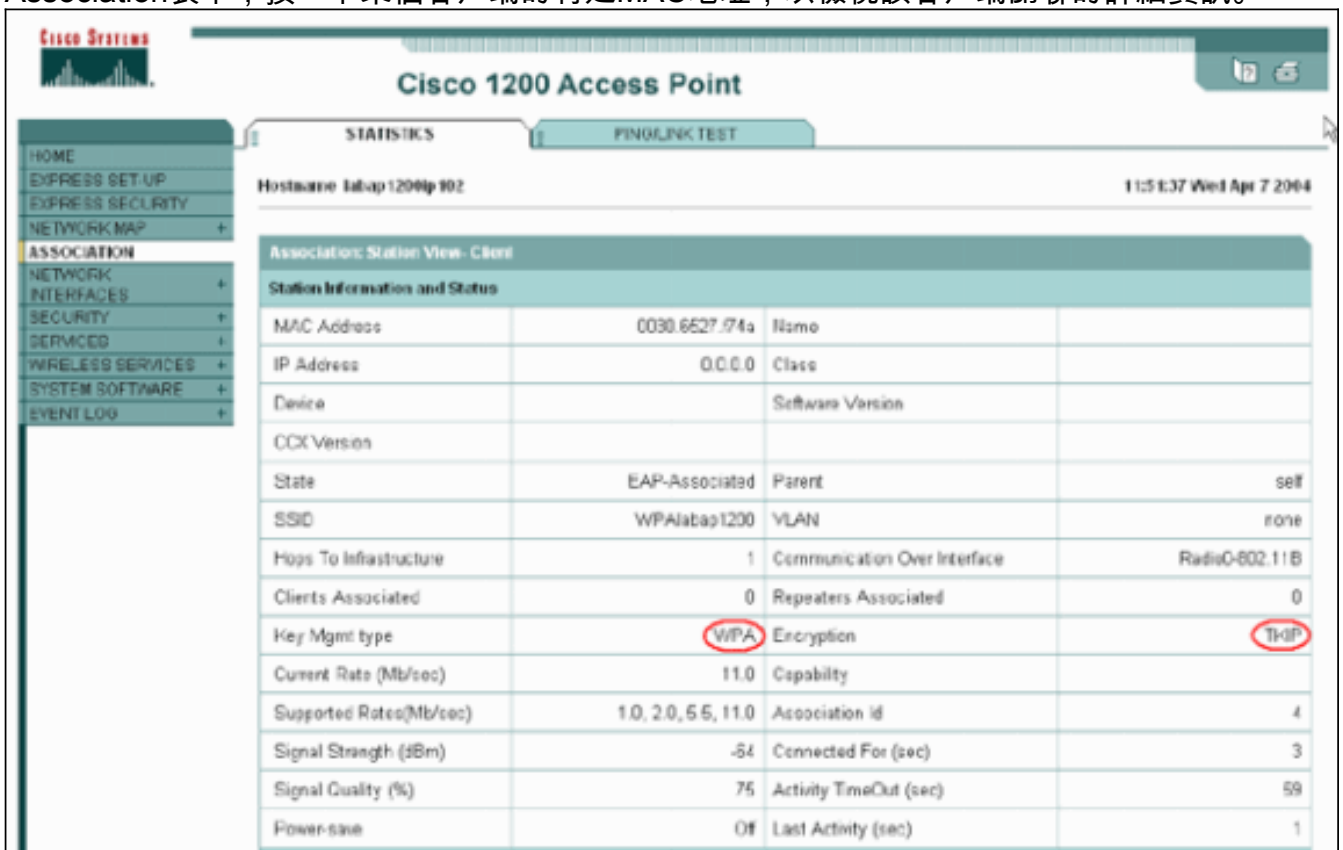
[輸出直譯器工具](#)(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析

。

- **show dot11 association mac\_address** — 此命令顯示有關特定標識的關聯客戶端的資訊。驗證客戶端是否將金鑰管理作為WPA協商，將加密作為TKIP。



- 特定客戶端的關聯表條目還必須將「金鑰管理」指示WPA，將「加密」指示TKIP。在 Association表中，按一下某個客戶端的特定MAC地址，以檢視該客戶端關聯的詳細資訊。



本節提供的資訊可用於對組態進行疑難排解。

## 疑難排解程式

此資訊與此組態相關。完成以下步驟，對組態進行疑難排解：

1. 如果此LEAP、EAP或PEAP配置在WPA實施之前尚未經過徹底測試，則必須完成以下步驟：  
：暫時禁用WPA加密模式。重新啟用適當的EAP。確認身份驗證有效。
2. 驗證客戶端的配置與AP的配置是否匹配。例如，當AP配置為WPA和TKIP時，確認設定與客戶端中配置的設定匹配。

## 指令疑難排解

附註：使用 `debug` 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

WPA金鑰管理涉及在EAP身份驗證成功完成後的四次握手。您可以在調試中看到這四條消息。如果EAP未成功驗證客戶端，或者您看不到消息，請完成以下步驟：

1. 暫時禁用WPA。
2. 重新啟用適當的EAP。
3. 確認身份驗證有效。

此清單說明偵錯專案：

- `debug dot11 aaa manager keys` — 此調試顯示AP和WPA客戶端之間發生的握手，作為成對臨時金鑰(PTK)和組臨時金鑰(GTK)協商。此偵錯是在Cisco IOS軟體版本12.2(15)JA中匯入。如果未顯示調試輸出，請驗證以下各項：終端監控術語`mon`已啟用（如果使用Telnet會話）。調試已啟用。客戶端已正確配置為WPA。如果調試顯示PTK和/或GTK握手已建立但未驗證，請檢查WPA請求方軟體是否正確配置和最新版本。
- `debug dot11 aaa authenticator state-machine` — 此調試顯示客戶端在關聯和身份驗證時經歷的各種協商狀態。狀態名稱表示這些狀態。此偵錯是在Cisco IOS軟體版本12.2(15)JA中匯入。`debug`取代Cisco IOS軟體版本12.2(15)JA和更新版本中的`debug dot11 aaa dot1x state-machine`命令。
- `debug dot11 aaa dot1x state-machine` — 此調試顯示客戶端在關聯和身份驗證時經歷的各種協商狀態。狀態名稱表示這些狀態。在低於Cisco IOS軟體版本12.2(15)JA的Cisco IOS軟體版本中，此偵錯也會顯示WPA金鑰管理交涉。
- `debug dot11 aaa authenticator process` — 此調試最有助於診斷協商通訊問題。詳細資訊顯示協商中的每個參與者傳送的内容，並顯示另一個參與者的響應。您還可以將此調試與`debug radius authentication`命令結合使用。此偵錯是在Cisco IOS軟體版本12.2(15)JA中匯入。`debug`取代Cisco IOS軟體版本12.2(15)JA和更新版本中的`debug dot11 aaa dot1x process`命令。
- `debug dot11 aaa dot1x process` — 此調試有助於診斷協商通訊的問題。詳細資訊顯示協商中的每個參與者傳送的内容，並顯示另一個參與者的響應。您還可以將此調試與`debug radius authentication`命令結合使用。在低於Cisco IOS軟體版本12.2(15)JA的Cisco IOS軟體版本中，此偵錯會顯示WPA金鑰管理交涉。

## 相關資訊

- [配置密碼套件和WEP](#)



- [配置身份驗證型別](#)
- [WPA2 - Wi-Fi保護訪問2](#)
- [Wi-Fi保護訪問2\(WPA 2\)配置](#)
- [技術支援與文件 - Cisco Systems](#)